ABSTRACT

An apparatus and method for generating pseudo-random cryptographic keys in a cryptographic communications systems, whereby, given a common set of initializing configuration data, the pseudo-random cryptographic keys can be duplicatively generated by various independent pseudo-random key generators of the cryptographic communications system.